MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017

TDF3241 – DIGITAL FORENSICS

(All Sections / Groups)

3 MARCH 2017
3:00 PM – 5:00 PM
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 pages (including cover page) with 5 Questions only.

2. Attempt **ALL** questions. The distribution of the marks for each question is given. This paper carries **50 marks**.

3. Please print all your answers in the Answer Booklet provided.

Question 1 (10 Marks)

a) Analyse and determine the best acquisition method to be used on large disks when your time is limited and justify your answer. [2 marks]

b) Briefly illustrate the steps required to create image files for digital evidence. [4 marks]

c) Break down the steps to examine the Windows registry by searching for specific key names based on a search term. [4 marks]

[TOTAL = 2 + 4 + 4 = 10]

Question 2 (10 Marks)

a) Categorise the main tasks performed by computer forensic tools into FIVE (5) categories. [5 marks]

b) You are required to conduct a forensics investigation. Compile a list of SIX (6) important activities you must perform in your strategy of conducting the investigation. [3 marks]

c) Categorise FOUR (4) areas of a mobile device which is involved in the mobile device acquisition process. [2 marks]

[TOTAL = 5 + 3 +2 = 10]

Continued ...

Question 3 (10 Marks)

Evidence Report for Project:

Project Number: 20160218_3

Project Description:

Image Files:
File Name: D:\HYL\Subjects\TDF3241-forensics\Labs\Labs\Lab 1\GCFI-Win98.eve
Image File Type: DFT Image
File Number: GCFI-Win98
Technician Name: Joe Friday
Date: 03/10/2007
Time: 15:51:34
Checksum: 736d1b2a054103d456e5fc6f0f8571b0
Checksum Validated: No
Compressed image: No
Time Zone Information:

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana (Pacific Standard Time)
Daylight savings (summertime) was in effect: Yes
Time Zone information obtained automatically from remote system/image.

Hard Disk: G:\
Volume Name: NO NAME
Volume Serial Number : 2367-1802
File System: FAT32
Bytes Per Sector: 512
Total Clusters: 68758
Sectors per cluster: 64
Total Sectors: 4401747
Hidden Sectors: 63
Total Capacity: 2200873 KB
Start Sector: 0
End Sector: 0

Disks:

Evidence of Interest:

Total Evidence Items of Interest: 6

Hard Disk: G:\
List of Files:

D:\HYL\Subjects\TDF3241-forensics\Labs\Labs\Lab 1\GCFI-Win98.eve\WINDOWS\Application Data\Identities\{95286EE0-564A-11D3-82D6-BF9664A29206}\Microsoft\Outlook Express\Inbox.dbx
MD5 Checksum: 084F31502952CDA6778711446F034A8C
Created: 01/27/2007 11:41 Modified: 02/14/2007 21:32 Last Accessed: 02/14/2007 00:00
MFT &STANDARD_INFO entry modified: Not available
MFT $FILE_NAME entry modified: Not available
Cluster Chain:
Fragmented File

Continued ...

Evaluate the report generated above:

a) Identify the program used to generate the report above. [2 marks]

b) Conclude FIVE (5) observations you can make about the file being analysed. *[Please do not include any answers related to Question 3(c)].* [5 marks]

c) Conclude THREE (3) possible countries the hard disk could have been seized from. [3 marks]

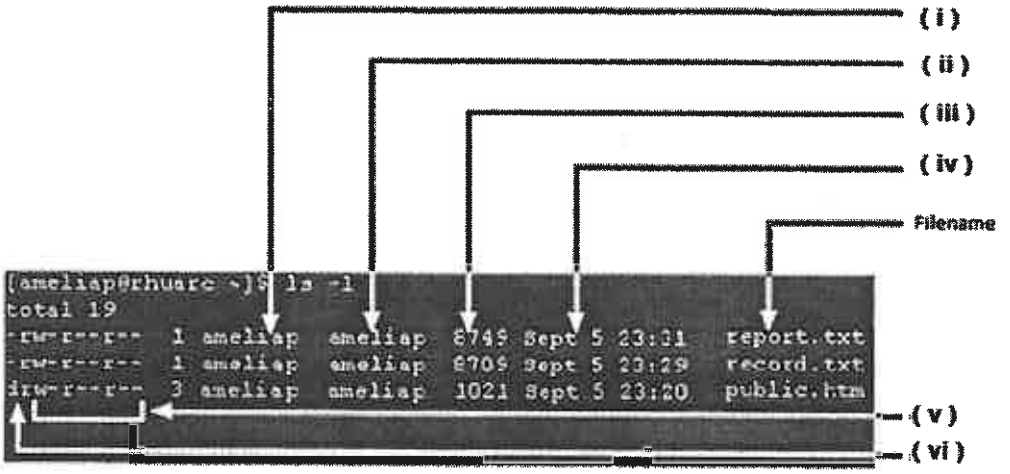
[TOTAL = 2 + 5 + 3 = 10]

Question 4 (10 Marks)

a) Distinguish FOUR (4) reconstruction functions in Guidance Software Encase. [2 marks]

b) Analyse the FOUR (4) main goals of forensic investigations. [2 marks]

c) Identify the following types of information found in a UNIX directory listing.



[6 marks]

[TOTAL = 2 + 2 + 6 = 10]

Continued ...

Question 5 (10 Marks)

a) Propose FOUR (4) standard procedures for network forensics. [4 marks]

b) Plan your steps in documenting and preparing evidence. Explain EIGHT (8) steps you would take to do so. [4 marks]

c) A verbal report addresses areas of investigation yet to be completed. Categorise these areas into FOUR (4) parts. [2 marks]

[TOTAL = 4 + 2 + 4 = 10]

END OF PAPER